

ENVIRONMENT

1/11

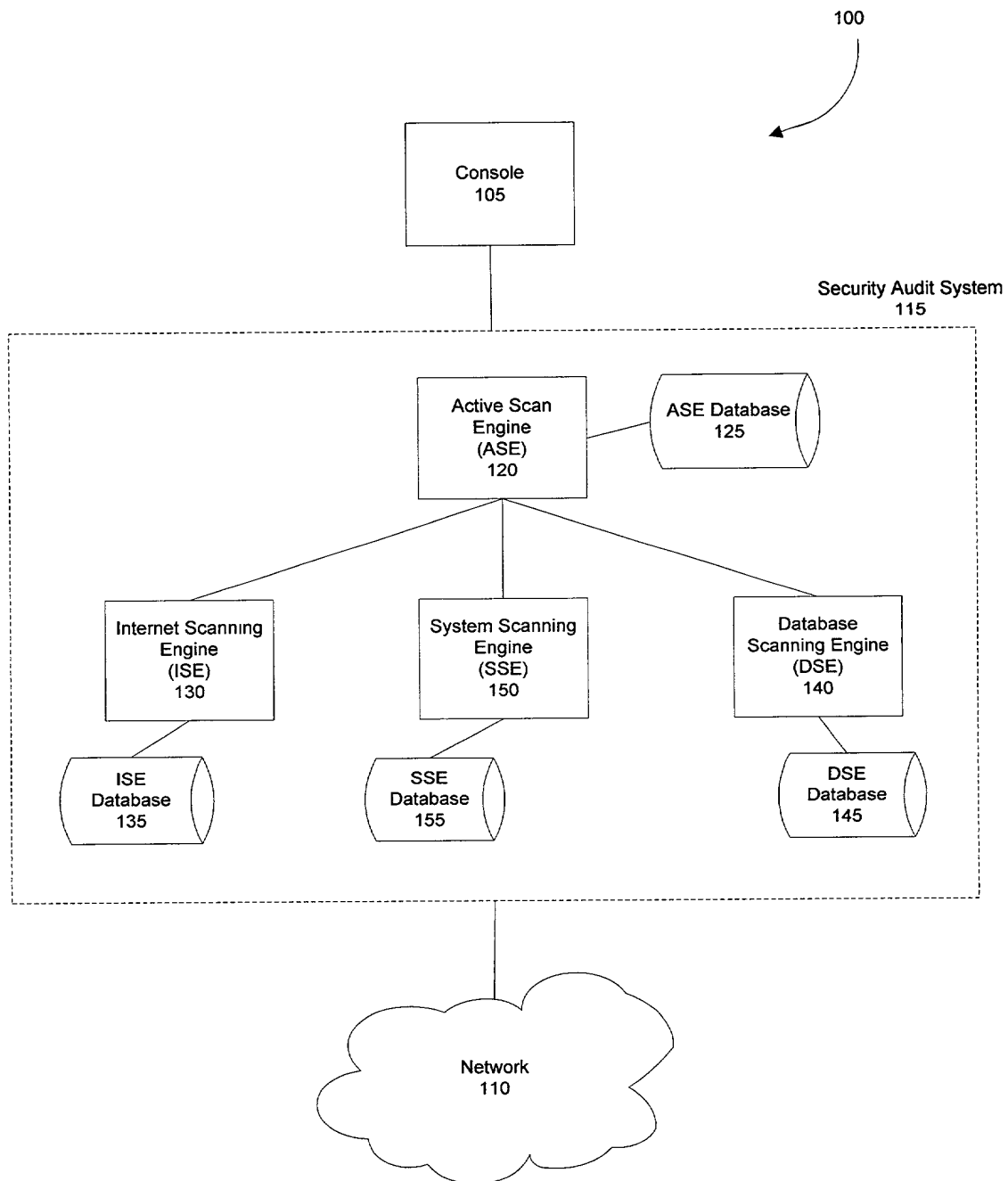


FIG. 1

OVERVIEW OF SECURITY AUDITING

2/11

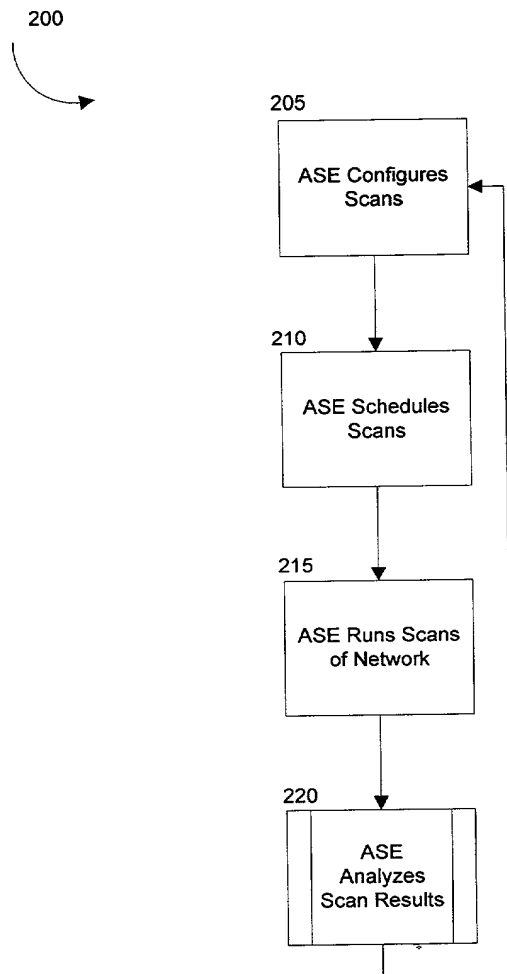
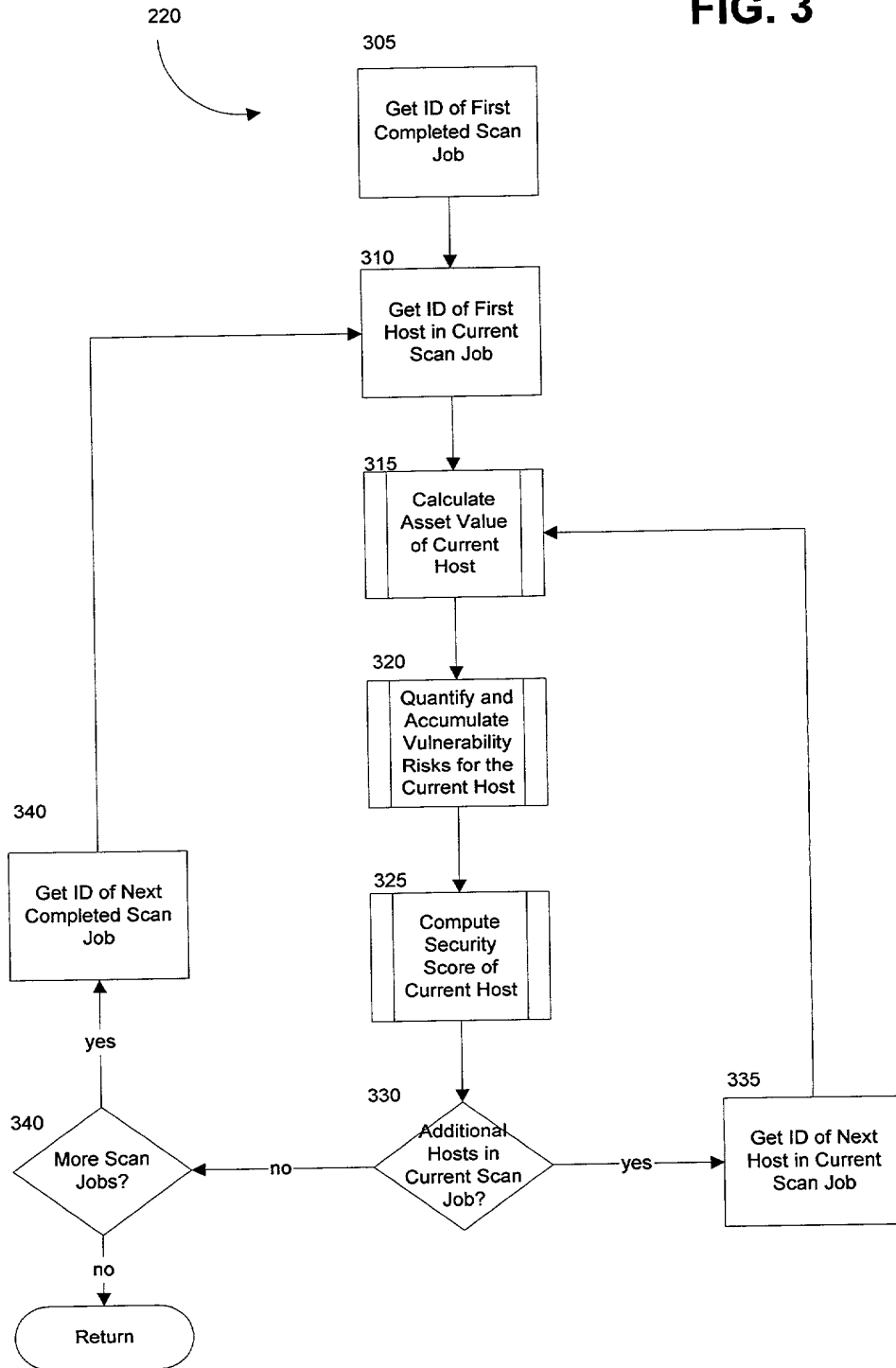


FIG. 2

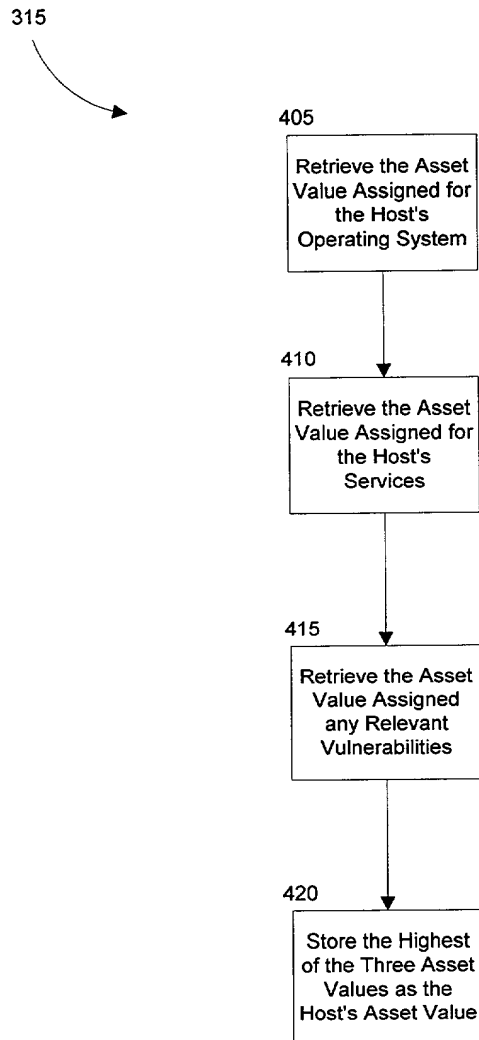
ANALYZE SCAN
RESULTS

3/11

FIG. 3



CALCULATE THE ASSET VALUE OF A HOST

**FIG. 4**

QUANTIFY AND ACCUMULATE
VULNERABILITY RISKS FOR A HOST

5/11

320

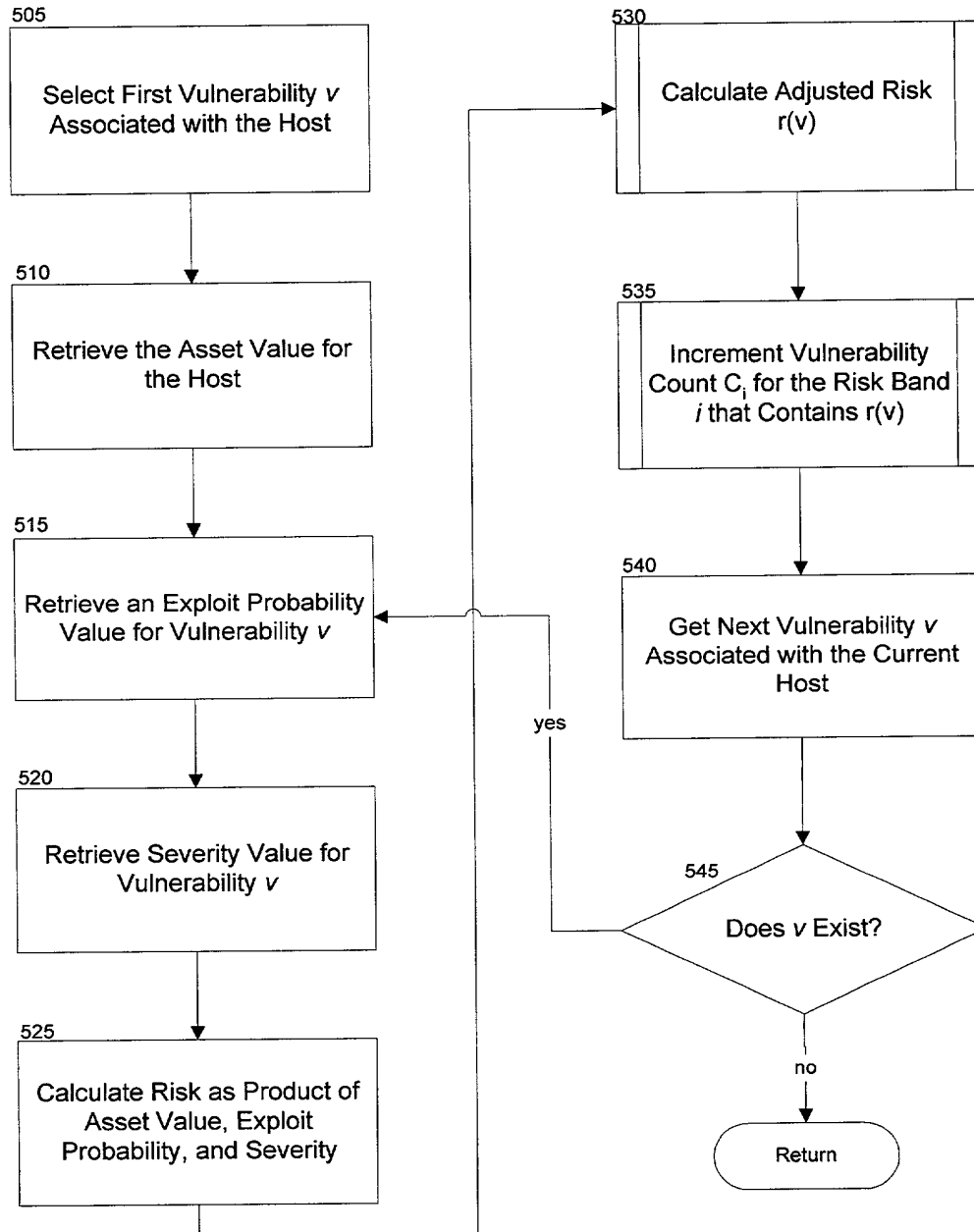


FIG. 5

CALCULATE
ADJUSTED RISK FOR A
VULNERABILITY

530

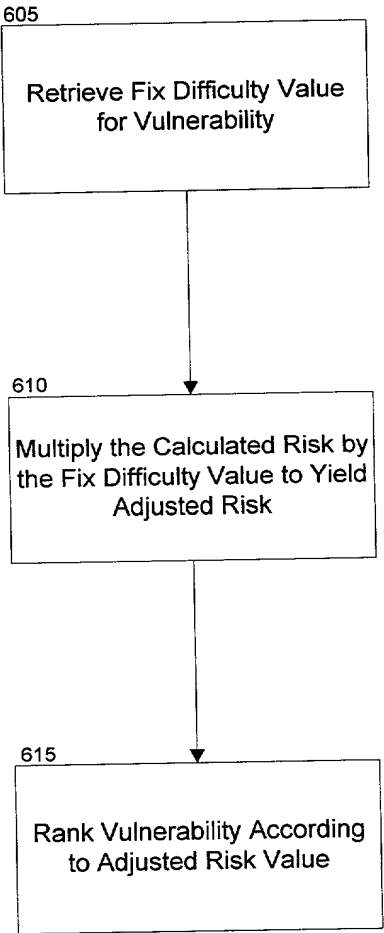


FIG. 6

INCREMENT
VULNERABILITY COUNT
 C_i FOR THE RISK BAND i
THAT CONTAINS RISK
 $r(v)$

535

705

Identify the band i such that
 $r_i \geq r(v) > r_{i-1}$

710

Increment the vulnerability
count C_i for band i by 1

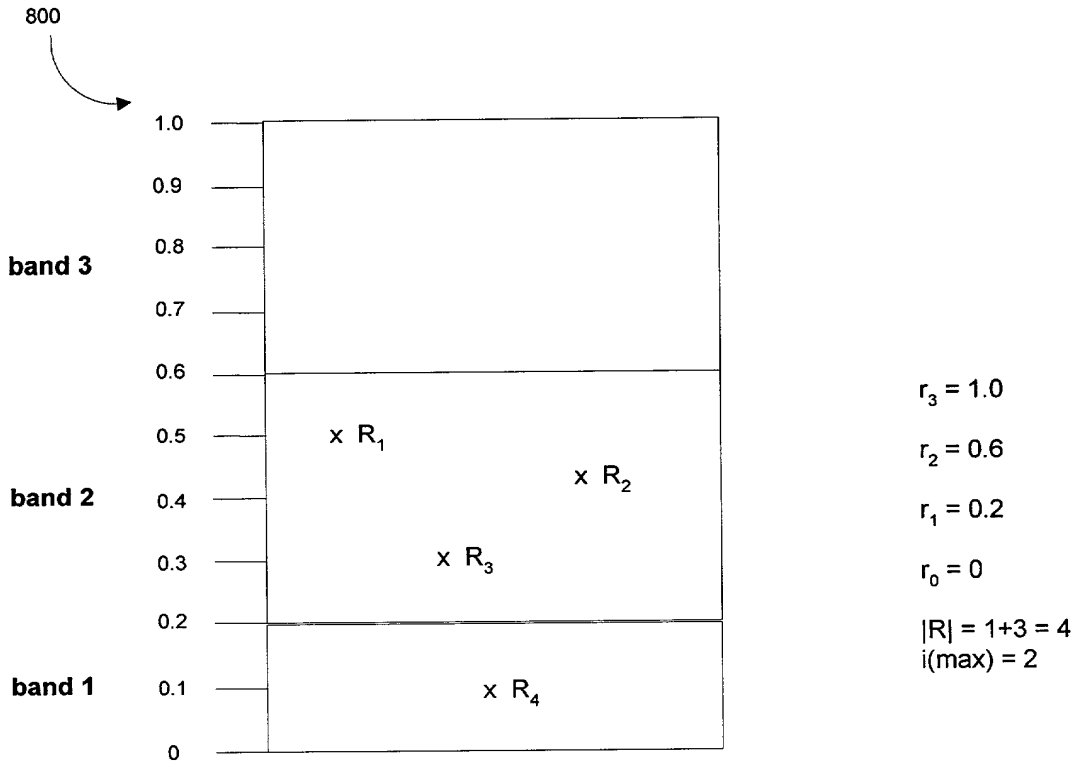
Notation:

- r_i = the maximum risk value of band i
- r_{i-1} = the maximum risk value of band $i - 1$
- $r(v)$ = the adjusted risk value of vulnerability v

FIG. 7

EXEMPLARY BAND CALCULATION

8/11



$$\text{Security Score} = r_{i(\max)-1} + \frac{r_{i(\max)} - r_{i(\max)-1}}{r_{i(\max)} + r_{i(\max)-1}} \sum_{k=1}^{|R|} \frac{r_{i(k)} + r_{i(k)-1}}{2^k}$$

Note:

Recognizing that the numerator ($r_{i(k)} + r_{i(k)-1}$) in the summation is constant for each band, and that

$$\sum_{k=i}^n \frac{1}{2^k} = \frac{2^{n-i+1} - 1}{2^n}$$

we can simplify the formula given above for computation purposes. The computations shown in subsequent figures implement the simplified method.

Notation:

- $i(\max)$ = the index of the highest-risk band with at least one vulnerability
- r_i = the risk value at the upper boundary of band i
- $i(k)$ = the index of the band that contains vulnerability k
- $|R|$ denotes the number of vulnerabilities on the host

FIG. 8A

COMPUTE A HOST'S
SECURITY SCORE

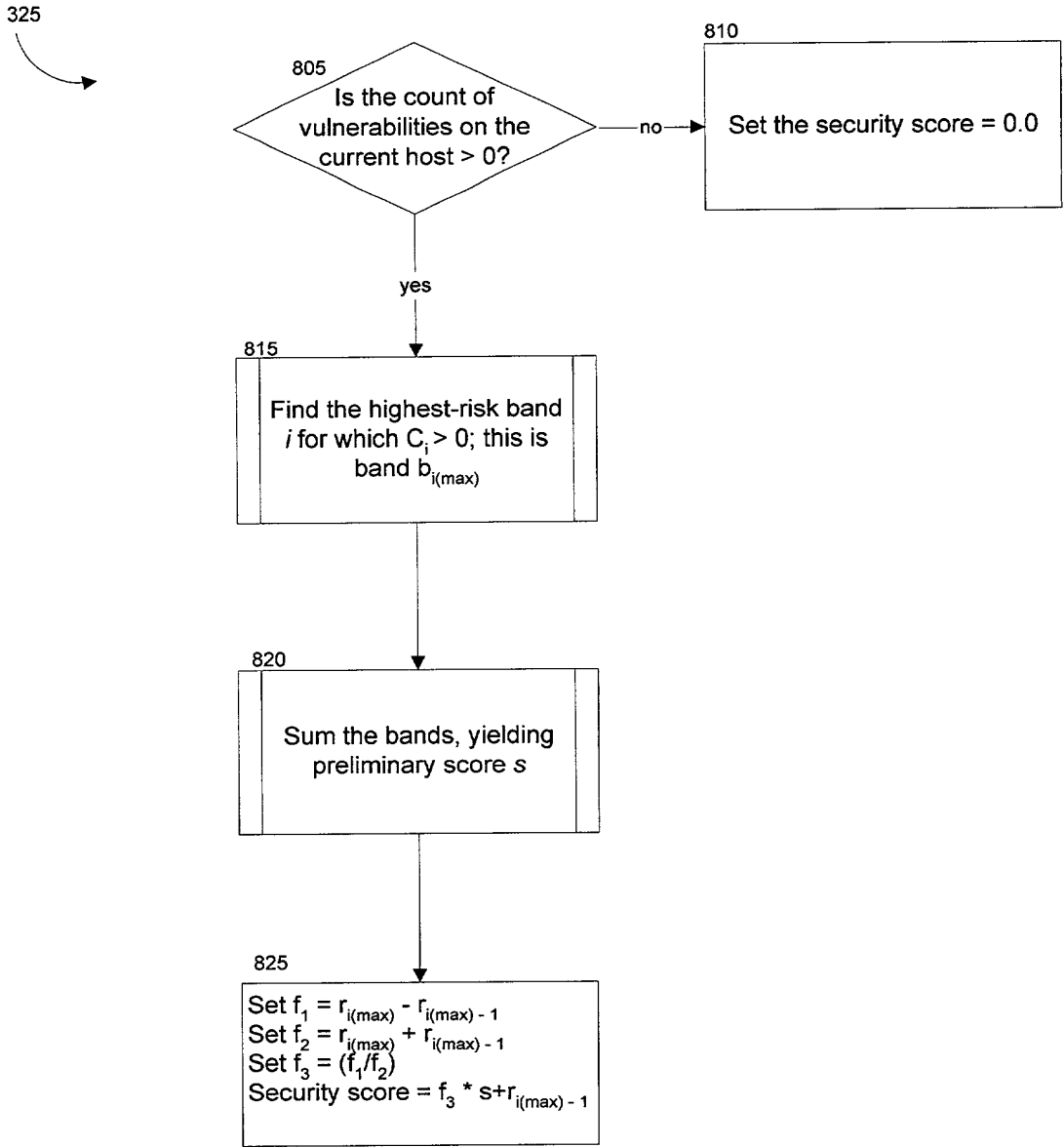


FIG. 8B

FIND THE HIGHEST-
RISK BAND i FOR
WHICH $C_i > 0$; THIS IS
BAND $b_{i(max)}$

10/11

815

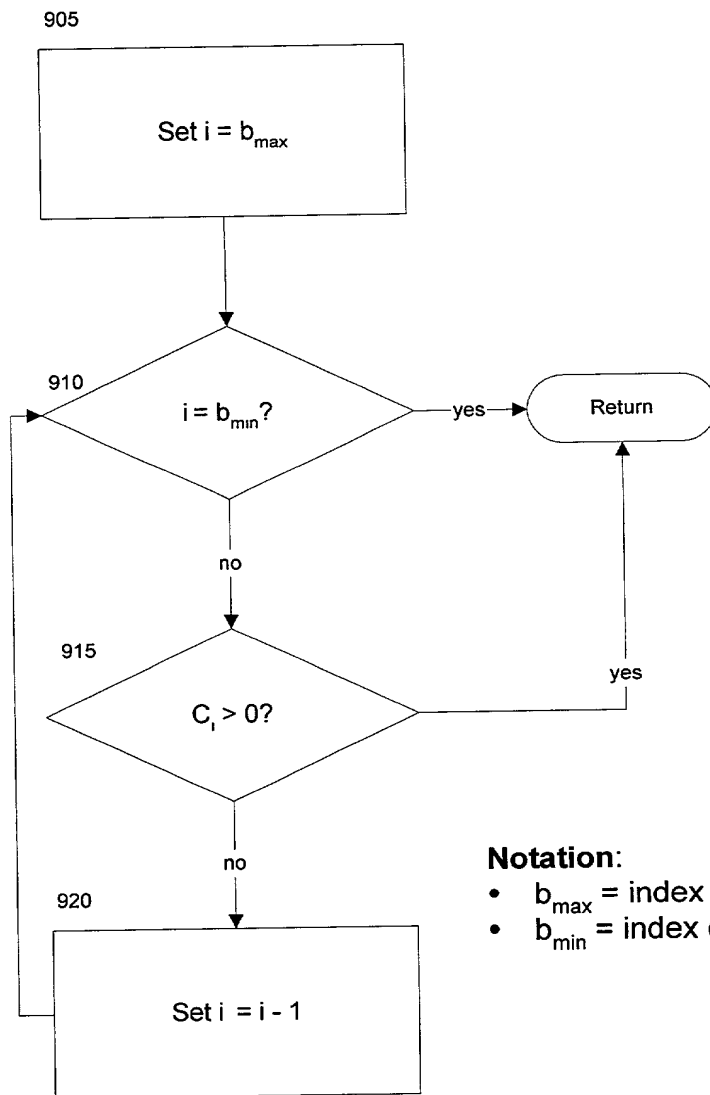


FIG. 9

SUM THE BANDS,
YIELDING
PRELIMINARY SCORE s

820



1005

Set $i = b_{i(max)}$
Set $s = 0.0$
Set PreviousCount = 0
Set StartIndex = 1

1010

$i \geq b_{min}?$

no

Return

yes

1015

Set $n = C_i + \text{PreviousCount}$
Set $s = s + (r_i + r_{i-1}) * (2^n - \text{StartIndex} + 1 - 1.0) / 2^n$
Set StartIndex = StartIndex + C_i
Set PreviousCount = PreviousCount + C_i
 $i = i - 1$

Notation:

- b_{min} = index of lowest-risk band
- $b_{i(max)}$ = index of highest-risk band with at least one vulnerability
- r_i = the maximum risk value of band i
- r_{i-1} = the maximum risk value of band $i - 1$

FIG. 10